明　細　書

量子鍵配送方法および通信装置

技術分野

本発明は、高度に安全性の保証された共通鍵を生成することが可能な量子鍵配送方法に関するものであり、特に、誤り訂正符号を用いてデータ誤りを訂正可能な量子鍵配送方法および当該量子鍵配送を実現可能な通信装置に関するものである。

背景技術

以下、従来の量子暗号システムについて説明する。近年、高速大容量な通信技術として光通信が広く利用されているが、このような光通信システムでは、光のオン／オフで通信が行われ、オンのときに大量の光子が送信されているため、量子効果が直接現れる通信系にはなっていない。

一方、量子暗号システムでは、通信媒体として光子を用い、不確定性原理等の量子効果が生じるように１個の光子で１ビットの情報を伝送する。このとき、盗聴者が、その偏光，位相等の量子状態を知らずに適当に基底を選んで光子を測定すると、その量子状態に変化が生じる。したがって、受信側では、この光子の量子状態の変化を確認することによって、伝送データが盗聴されたかどうかを認識することができる。

第１０図は、従来の偏光を利用した量子鍵配送の概要を示す図である。たとえば、水平垂直方向の偏光を識別可能な測定器では、量子通信路上の、水平方向（０°）に偏光された光と垂直方向（９０°）に偏光された光とを正しく識別する。一方、斜め方向（４５°，１３５°）の偏光を識別可能な測定器では、量子通信路上の、４５°方向に偏光された光と１３５°方向に偏光された光とを正しく識別する。

このように、各測定器は、規定された方向に偏光された光については正しく認識できるが、たとえば、斜め方向に偏光された光を水平垂直方向（０°，９０°）の偏光を識別可能な測定器にて測定すると、水平方向と垂直方向に偏光された光をそれぞれ５０％の確率でランダムに識別する。すなわち、識別可能な偏光方向に対応していない測定器を用いた場合には、その測定結果を解析しても、偏光された方向を正しく識別することができない。

第１０図に示す従来の量子鍵配送では、上記不確定性（ランダム性）を利用して、盗聴者に知られずに送信者と受信者との間で鍵を共有する（たとえば、非特許文献１参照。）。なお、送信者および受信者は、量子通信路以外に公開通信路を使用することができる。

ここで、鍵の共有手順について説明する。まず、送信者は、乱数列（１，０の列：送信データ）を発生し、さらに送信コード（＋：水平垂直方向に偏光された光を識別可能な測定器に対応，×：斜め方向に偏光された光を識別可能な測定器に対応）をランダムに決定する。その乱数列と送信コードの組み合わせで、送信する光の偏光方向が自動的にきまる。ここでは、０と＋の組み合わせで水平方向に偏光された光を、１と＋の組み合わせで垂直方向に偏光された光を、０と×の組み合わせで４５° 方向に偏光された光を、１と×の組み合わせで１３５° 方向に偏光された光を、量子通信路にそれぞれ送信する（送信信号）。

つぎに、受信者は、受信コード（＋：水平垂直方向に偏光された光を識別可能な測定器，× ：斜め方向に偏光された光を識別可能な測定器）をランダムに決定し、量子通信路上の光を測定する（受信信号）。そして、受信コードと受信信号の組み合わせによって受信データを得る。ここでは、受信データとして、水平方向に偏光された光と＋の組み合わせで０を、垂直方向に偏光された光と＋の組み合わせで１を、４５° 方向に偏光された光と×の組み合わせで０を、１３５° 方向に偏光された光と×の組み合わせで１を、それぞれ得る。

つぎに、受信者は、自身の測定が正しい測定器で行われたものかどうかを調べるために、受信コードを、公開通信路を介して送信者に対して送信する。受信コ

ードを受け取った送信者は、正しい測定器で行われたものかどうかを調べ、その結果を、公開通信路を介して受信者に対して返信する。

つぎに、受信者は、正しい測定器で受信した受信信号に対応する受信データだけを残し、その他を捨てる。この時点で、残された受信データは送信者と受信者との間で確実に共有できている。

つぎに、送信者と受信者は、それぞれの通信相手に対して、共有データから選択した所定数のデータを、公開通信路を経由して送信する。そして、受け取ったデータが自身の持つデータと一致しているかどうかを確認する。たとえば、確認したデータの中に一致しないデータが１つでもあれば、盗聴者がいるものと判断して共有データを捨て、再度、鍵の共有手順を最初からやり直す。一方、確認したデータがすべて一致した場合には、盗聴者がいないと判断し、確認に使用したデータを捨て、残った共有データを送信者と受信者の共有鍵とする。

一方、上記従来の量子鍵配送方法の応用として、たとえば、伝送路上におけるデータ誤りを訂正可能な量子鍵配送方法がある（たとえば、非特許文献２参照。）。

この方法では、送信者が、データ誤りを検出するために、送信データを複数のブロックに分割し、ブロック毎のパリティを公開通信路上に送信する。そして、受信者が、公開通信路を経由して受け取ったブロック毎のパリティと受信データにおける対応するブロックのパリティとを比較して、データ誤りをチェックする。このとき、異なるパリティがあった場合、受信者は、どのブロックのパリティが異なっているのかを示す情報を公開通信路上に返信する。そして、送信者は、該当するブロックをさらに前半部のブロックと後半部のブロックに分割し、たとえば、前半部のパリティを公開通信路上に返信する（二分探索）。以降、送信者と受信者は、上記二分探索を繰り返し実行することによりエラービットの位置を特定し、最終的に受信者がそのビットを訂正する。

さらに、送信者は、データに誤りがあるにもかかわらず、偶数個の誤りのために正しいと判定されたパリティがある場合を想定し、送信データをランダムに並

べ替えて（ランダム置換）複数のブロックに分割し、再度、上記二分探索による誤り訂正処理を行う。そして、ランダム置換によるこの誤り訂正処理を繰り返し実行することによって、すべてのデータ誤りを訂正する。

非特許文献１.

Bennett, C. H. and Brassard, G.: Quantum Cryptography: PublicKey Distribution and Coin Tossing, In Proceedings of IEEE Conference onComputers, System and Signal Processing, Bangalore, India, pp.175-179 (DEC.1984).

非特許文献２.

Brassard, G. and Salvail, L. 1993 Secret-Key Reconciliation by Public Discussion, In Advances in Cryptology - EUROCRYPT'93, Lecture Notes in Computer Science 765, 410-423.

しかしながら、上記第１０図に示す従来の量子鍵配送においては、誤り通信路を想定していないため、誤りがある場合には盗聴行為が存在したものとして上記共通データ（共通鍵）を捨てることとなり、伝送路によっては共通鍵の生成効率が非常に悪くなる、という問題があった。

また、上記伝送路上におけるデータ誤りを訂正可能な量子鍵配送方法においては、エラービットを特定するために膨大な回数のパリティのやりとりが発生し、さらに、ランダム置換による誤り訂正処理が所定回数にわたって行われるため、誤り訂正処理に多大な時間を費やすことになる、という問題があった。

本発明は、上記に鑑みてなされたものであって、極めて高い特性を持つ誤り訂正符号を用いて伝送路上におけるデータ誤りを訂正しつつ、高度に安全性の保証された共通鍵を生成することが可能な量子鍵配送方法を提供することを目的とする。

発明の開示

本発明にかかる量子鍵配送方法は、暗号鍵の元となる乱数列を所定の量子状態

で量子通信路上に送信する送信側の通信装置と、当該量子通信路上の光子を測定する受信側の通信装置、で構成された量子暗号システムにおける量子鍵配送方法であって、たとえば、各通信装置が、同一のパリティ検査行列（要素が「０」または「１」の行列）を生成する検査行列生成ステップ（後述する実施の形態のステップＳ１，Ｓ１１に相当）と、前記送信側の通信装置が、誤り検出のための巡回符号（ＣＲＣ：Cyclic Redundancy check）を生成する巡回符号生成ステップ（ステップＳ２に相当）と、前記受信側の通信装置が、光方向を正しく識別可能な測定器で測定した結果として得られた確率情報付きの受信データを保持し、前記送信側の通信装置が、前記受信データに対応する送信データ（乱数列の一部）を保持する送受信ステップ（ステップＳ３，Ｓ４，Ｓ１２，Ｓ１３に相当）と、前記送信側の通信装置が、前記パリティ検査行列および前記送信データに基づいて生成した誤り訂正情報と、前記巡回符号および前記送信データに基づいて生成した誤り検出情報と、を公開通信路を介して前記受信側の通信装置に通知する情報通知ステップ（ステップＳ５，Ｓ１４に相当）と、前記受信側の通信装置が、前記パリティ検査行列と前記確率情報付きの受信データと前記誤り訂正情報と前記誤り検出情報に基づいて、前記送信データを推定する送信データ推定ステップ（ステップＳ１５に相当）と、前記各通信装置が、公開された情報量に応じて送信データの一部を捨てて、残りの情報で暗号鍵を生成する暗号鍵生成ステップ（ステップＳ６，Ｓ１６に相当）と、を含むことを特徴とする。

この発明によれば、たとえば、確定的で特性が安定した「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」用のパリティ検査行列を用いて共有情報のデータ誤りを訂正し、さらに、巡回符号ＣＲＣを用いて共有情報（推定語）の誤り検出を行い、その後、公開された誤り訂正情報に応じて共有情報の一部を捨てることとした。

図面の簡単な説明

第１図は、本発明にかかる量子暗号システム（送信側および受信側の通信装置）の構成を示す図であり、第２図は、量子鍵配送の概要を示すフローチャートで

あり、第３図は、量子鍵配送の概要を示すフローチャートであり、第４図は、有限アフィン幾何に基づく「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」の構成法を示すフローチャートであり、第５図は、有限アフィン幾何符号ＡＧ（２，2^2）のマトリクスを示す図であり、第６図は、最終的な列の重み配分λ（γ_i）と行の重み配分ρ_uを示す図であり、第７図は、巡回符号ＣＲＣ（ｎ×ｄ行列）の一例を示す図であり、第８図は、m_AのシンドロームＳ$_A$および巡回符号シンドロームＳ$_c$の生成方法の概略構成を示す図であり、第９図は、本実施の形態のシンドローム復号法を示すフローチャートであり、第１０図は、従来の偏光を利用した量子鍵配送の概要を示す図である。

発明を実施するための最良の形態

以下に、本発明にかかる量子鍵配送方法の実施の形態を図面に基づいて詳細に説明する。なお、この実施の形態によりこの発明が限定されるものではない。また、以下では、例として偏光を利用する量子鍵配送について説明するが、本発明は、たとえば、位相を利用するもの，周波数を利用するもの等にも適用可能であり、どのような量子状態を利用するかについては特に限定しない。

量子鍵配送は、盗聴者の計算能力によらず、安全性の保証された鍵配送方式であるが、たとえば、より効率よく共有鍵を生成するためには、伝送路を通ることによって発生するデータの誤りを取り除く必要がある。そこで、本実施の形態では、極めて高い特性をもつことが知られている低密度パリティ検査（ＬＤＰＣ：：Low-Density Parity-Check）符号を用いて誤り訂正を行う量子鍵配送について説明する。

第１図は、本発明にかかる量子暗号システム（送信側および受信側の通信装置）の構成を示す図である。この量子暗号システムは、情報m_aを送信する機能を備えた送信側の通信装置と、伝送路上で雑音等の影響を受けた情報m_a、すなわち情報m_bを受信する機能を備えた受信側の通信装置と、から構成される。

また、送信側の通信装置は、量子通信路を介して情報m_aを送信し、公開通信路

を介してシンドロームＳ$_A$を送信し、これらの送信情報に基づいて暗号鍵（受信側との共通鍵）を生成する暗号鍵生成部１と、暗号化部２１が暗号鍵に基づいて暗号化したデータを、送受信部２２が公開通信路を介してやりとりする通信部２と、を備え、受信側の通信装置は、量子通信路を介して情報m_bを受信し、公開通信路を介してシンドロームＳ$_A$を受信し、これらの受信情報に基づいて暗号鍵（送信側との共通鍵）を生成する暗号鍵生成部３と、暗号化部４２が暗号鍵に基づいて暗号化したデータを、送受信部４１が公開通信路を介してやりとりする通信部４と、を備える。

上記送信側の通信装置では、量子通信路上に送信する情報m_aとして、偏光フィルターを用いて所定の方向に偏光させた光を、受信側の通信装置に対して送信する。一方、受信側の通信装置では、水平垂直方向（０°，９０°）の偏光を識別可能な測定器と斜め方向（４５°，１３５°）の偏光を識別可能な測定器とを用いて、量子通信路上の、水平方向（０°）に偏光された光と垂直方向（９０°）に偏光された光と４５°方向に偏光された光と１３５°方向に偏光された光とを識別する。なお、各測定器は、規定された方向に偏光された光については正しく認識できるが、たとえば、斜め方向に偏光された光を水平垂直方向（０°，９０°）の偏光を識別可能な測定器にて測定すると、水平方向と垂直方向に偏光された光をそれぞれ５０％の確率でランダムに識別する。すなわち、識別可能な偏光方向に対応していない測定器を用いた場合には、その測定結果を解析しても、偏光された方向を正しく識別することができない。

以下、上記量子暗号システムにおける各通信装置の動作、すなわち、本実施の形態における量子鍵配送について詳細に説明する。第２図および第３図は、本実施の形態の量子鍵配送の概要を示すフローチャートであり、詳細には、第２図は送信側の通信装置の処理を示し、第３図は受信側の通信装置の処理を示す。

まず、上記送信側の通信装置および受信側の通信装置では、パリティ検査行列生成部１０，３０が、特定の線形符号のパリティ検査行列Ｈ（ｎ×ｋ行列）を求め、このパリティ検査行列Ｈから「ＨＧ＝０」を満たす生成行列Ｇ（（ｎ－ｋ）

・×ｎ行列）を求め、さらに、G^{-1}・Ｇ＝Ｉ（単位行列）となるＧの逆行列G^{-1}（ｎ×（ｎ－ｋ）行列）を求める（ステップＳ１，ステップＳ１１）。本実施の形態では、上記特定の線形符号として、シャノン限界に極めて近い優れた特性をもつＬＤＰＣ符号を用いた場合の量子鍵配送について説明する。なお、本実施の形態では、誤り訂正方式としてＬＤＰＣ符号を用いることとしたが、これに限らず、たとえば、ターボ符号等の他の線形符号を用いることとしてもよい。また、たとえば、後述する誤り訂正情報（シンドローム）が適当な行列Ｈと送信データm_A（情報m_aの一部）の積Ｈm_Aで表される誤り訂正プロトコル（たとえば、従来技術にて説明した「伝送路上におけるデータ誤りを訂正可能な量子鍵配送」に相当する誤り訂正プロトコル）であれば、すなわち、誤り訂正情報と送信データm_Aの線形性が確保されるのであれば、その行列Ｈをパリティ検査行列として用いることとしてもよい。

ここで、上記パリティ検査行列生成部１０におけるＬＤＰＣ符号の構成法について、詳細には、有限アフィン幾何に基づく「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」の構成法（第２図ステップＳ１の詳細）について説明する。第４図は、有限アフィン幾何に基づく「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」の構成法を示すフローチャートである。なお、パリティ検査行列生成部３０については、パリティ検査行列生成部１０と同様に動作するのでその説明を省略する。また、本実施の形態における検査行列生成処理は、たとえば、設定されるパラメータに応じてパリティ検査行列生成部１０で実行する構成としてもよいし、通信装置外部の他の制御装置（計算機等）で実行することとしてもよい。本実施の形態における検査行列生成処理が通信装置外部で実行される場合は、生成済みの検査行列が通信装置に格納される。以降の実施の形態では、パリティ検査行列生成部１０で上記処理を実行する場合について説明する。

まず、パリティ検査行列生成部１０では、「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」用の検査行列のベースとなる有限アフィン幾何符号ＡＧ（２，2^s）を選択する（第４図、ステップＳ２１）。ここでは、行の重みと列の重みがそれぞれ2^s

となる。第５図は、たとえば、有限アフィン幾何符号ＡＧ（２，２^2）のマトリクスを示す図（空白は０を表す）である。

つぎに、パリティ検査行列生成部１０では、列の重みの最大値r_1（$2<r_1\leqq 2^s$）を決定する（ステップＳ２２）。そして、符号化率ｒａｔｅ（１シンドローム長／鍵の長さ）を決定する（ステップＳ２２）。

つぎに、パリティ検査行列生成部１０では、ガウス近似法（Gaussian Approximation）による最適化を用いて、暫定的に、列の重み配分λ（γ_i）と行の重み配分ρ_uを求める（ステップＳ２３）。なお、行の重み配分の生成関数ρ（ｘ）はρ（ｘ）＝$\rho_u x^{u-1}+(1-\rho_u)\,x^u$とする。また、重みｕはｕ≧２の整数であり、$\rho_u$は行における重みｕの割合を表す。

つぎに、パリティ検査行列生成部１０では、有限アフィン幾何の行の分割により構成可能な、行の重み｛ｕ，ｕ＋１｝を選択し、さらに（１）式を満たす分割係数｛b_u，b_{u+1}｝を求める（ステップＳ２４）。なお、b_u，b_{u+1}は非負の整数とする。

$$b_u+b_{u+1}(u+1)=2^s \qquad \cdots(1)$$

具体的には、下記（２）式からb_uを求め、上記（１）式からb_{u+1}を求める。

$$\arg\cdot\min_{bu}\left|\varphi_u-\frac{u\times b_u}{2^s}\right| \qquad \cdots(2)$$

つぎに、パリティ検査行列生成部１０では、上記決定したパラメータｕ，ｕ＋１，b_u，b_{u+1}によって更新された行の重みの比率ρ_u'，ρ_{u+1}'を（３）式により求める（ステップＳ２５）。

$$\varphi_u'=\frac{u\times b_u}{2^s}$$
$$\varphi_{u+1}'=\frac{(u+1)\times b_{u+1}}{2^s} \qquad \cdots(3)$$

つぎに、パリティ検査行列生成部１０では、ガウス近似法による最適化を用いて、さらに上記で求めたｕ，ｕ＋１，ρ_u´，ρ_{u+1}´を固定のパラメータとして、暫定的に、列の重み配分λ（γ_i）を求める（ステップＳ２６）。なお、重みγ_iは$\gamma_i \geqq 2$の整数であり、λ（γ_i）は列における重みγ_iの割合を表す。また、列数が１以下となる重み（λ（γ_i）$\leqq \gamma_i / w_t$，ｉは正の整数）を候補から削除する。ただし、w_tはＡＧ（２，2^s）に含まれる１の総数を表す。

つぎに、上記で求めた重み配分を満たし、かつ下記（４）式を満たす、列の重み候補のセット｛γ_1，γ_2，…γ_l（$\gamma_l \leqq 2^s$）｝を選択する（ステップＳ２７）。そして、下記の（４）式を満たさない列の重みγ_iが存在する場合には、その列の重みを候補から削除する。

$$\begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,\ell} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,\ell} \\ \vdots & & \cdots & \vdots \end{bmatrix} \begin{bmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_\ell \end{bmatrix} = \begin{bmatrix} 2^s \\ 2^s \\ \vdots \\ 2^s \end{bmatrix} \quad \cdots (4)$$

なお、各ａは、列の重み2^sを構成するための｛γ_1，γ_2，…γ_l｝に対する非負の整数となる係数を表し、ｉ，ｊは正の整数であり、γ_iは列の重みを表し、γ_1は列の最大重みを表す。

つぎに、パリティ検査行列生成部１０では、ガウス近似法による最適化を用いて、さらに上記で求めたｕ，ｕ＋１，ρ_u´，ρ_{u+1}´と｛γ_1，γ_2，…γ_l｝を固定パラメータとして、列の重み配分λ（γ_i）と行の重み配分ρ_uを求める（ステップＳ２８）。

つぎに、パリティ検査行列生成部１０では、分割処理を行う前に、列の重み配分λ（γ_i）と行の重み配分ρ_uを調整する（ステップＳ２９）。なお、調整後の各重みの配分は、可能な限りガウス近似法で求めた値に近い値にする。第６図は、ステップＳ２９における最終的な列の重み配分λ（γ_i）と行の重み配分ρ_uを示

す図である。なお、ｎ（γ_i）は、重み単位の総列数を表し、n_uは重み単位の総行数を表す。

最後に、パリティ検査行列生成部１０では、有限アフィン幾何における行および列を分割して（ステップＳ３０）、ｎ×ｋのパリティ検査行列Ｈを生成する。本発明における有限アフィン幾何符号の分割処理は、規則的に分割するのではなく、各行または各列から「１」をランダムに抽出する。なお、この抽出処理は、ランダム性が保持されるのであればどのような方法を用いてもよい。

このように、本実施の形態では、上記有限アフィン幾何に基づく「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」の構成法（第２図、ステップＳ１）を実行することによって、確定的で特性が安定した「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」用の検査行列Ｈ（ｎ×ｋ行列）を生成することができる。

上記のように、パリティ検査行列Ｈ（ｎ×ｋ行列），生成行列Ｇ，G^{-1}（G^{-1}・Ｇ＝Ｉ：単位行列）を生成後、つぎに、送信側の通信装置では、受信側の通信装置が送信データm_Aを正確に推定できない可能性（送信データm_Aと後述する推定語m_Cが一致しない場合）があるので、特に、盗聴者の存在により誤判定の発生確率が高くなる場合があるので、このような誤判定確率を極力小さくするために、巡回符号生成部１６にて、誤り検出のための巡回符号ＣＲＣ（Cyclic Redundancy check）を生成する（第２図、ステップＳ２）。ここでは、上記で生成したパリティ検査行列Ｈとは別に、巡回符号ＣＲＣ（ｎ×ｄ行列）を生成する。

ここで、上記巡回符号生成部１６における巡回符号ＣＲＣ（ｎ×ｄ行列）の構成法（第２図ステップＳ２の詳細）について説明する。

たとえば、鍵長ｎをｎ＝７とし、ＧＦ（２）上の原始多項式ｇｘを多項式表現したときの最大次数ｄをｄ＝３とし、３次の原始多項式ｇｘを$g(x)=x^3+x+1$（ベクトル表現：［１０１１］）とした場合（ｎ×ｄのＣＲＣを構成する場合）、ＣＲＣの検査多項式$x^{d-1}H(x^{-1})$は下記（５）式のように表すことができる。なお、多項式Ｈ（ｘ）は、$H(x)=(x^n+1)/g(x)$である。

$$H(x)=(x^n+1)/g(x)$$

$= (x^7+1) / (x^3+x+1)$

$= x^4+x^2+x+1$ （ベクトル表現：［１０１１１］）

$H(x^{-1}) = x^{-4}+x^{-2}+x^{-1}+1$

$= x^4+x^3+x^2+1$ （ベクトル表現：［１１１０１］）

$x^{d-1}H(x^{-1}) = x^2 \times (x^4+x^3+x^2+1)$

$= x^6+x^5+x^4+x^2$ （ベクトル表現：［１１１０１００］）

… (5)

したがって、巡回符号ＣＲＣ（ｎ×ｄ行列）は、ＣＲＣの検査多項式$x^{d-1}H(x^{-1})$のベクトル表現：［１１１０１００］を巡回シフト（ｄ＝３）した、第７図に示すｎ×ｄの行列となる。第７図は、巡回符号ＣＲＣ（ｎ×ｄ行列）の一例を示す図である。

上記のように、巡回符号ＣＲＣ（ｎ×ｋ行列）を生成後、つぎに、送信側の通信装置では、乱数発生部１１が、乱数列m_a（１，０の列：送信データ）を発生し、さらに送信コード（＋：水平垂直方向に偏光された光を識別可能な測定器に対応したコード，×：斜め方向に偏光された光を識別可能な測定器に対応したコード）をランダムに決定する（第２図、ステップＳ３）。一方、受信側の装置では、乱数発生部３１が、受信コード（＋：水平垂直方向に偏光された光を識別可能な測定器に対応したコード，×：斜め方向に偏光された光を識別可能な測定器に対応したコード）をランダムに決定する（第３図、ステップＳ１２）。

つぎに、送信側の通信装置では、光子生成部１２が、上記乱数列m_aと送信コードの組み合わせで自動的に決まる偏光方向で光子を送信する（ステップＳ４）。たとえば、０と＋の組み合わせで水平方向に偏光された光を、１と＋の組み合わせで垂直方向に偏光された光を、０と×の組み合わせで４５°方向に偏光された光を、１と×の組み合わせで１３５°方向に偏光された光を、量子通信路にそれぞれ送信する（送信信号）。

光子生成部１２の光信号を受け取った受信側の通信装置の光子受信部３２では、量子通信路上の光を測定する（受信信号）。そして、受信コードと受信信号の組

み合わせによって自動的に決まる受信データm_bを得る（ステップＳ１３）。ここでは、受信データm_bとして、水平方向に偏光された光と＋の組み合わせで０を、垂直方向に偏光された光と＋の組み合わせで１を、４５° 方向に偏光された光と×の組み合わせで０を、１３５° 方向に偏光された光と×の組み合わせで０を、それぞれ得る。なお、受信データm_bは、確率情報付きの硬判定値とする。

つぎに、受信側の通信装置では、上記測定が正しい測定器で行われたものかどうかを調べるために、乱数発生部３１が、受信コードを、公開通信路を介して送信側の通信装置に対して送信する（ステップＳ１３）。受信コードを受け取った送信側の通信装置では、上記測定が正しい測定器で行われたものかどうかを調べ、その結果を、公開通信路を介して受信側の通信装置に対して送信する（ステップＳ４）。そして、受信側の通信装置および送信側の通信装置では、正しい測定器で受信した受信信号に対応するデータだけを残し、その他を捨てる（ステップＳ４，Ｓ１３）。その後、残ったデータをメモリ等に保存し、その先頭から順にｎビットを読み出し、これを、正式な送信データm_Aと受信データm_B（m_Bは伝送路上で雑音等の影響を受けたm_A：$m_B=m_A+e$（雑音等））とする。すなわち、ここでは、必要に応じてつぎのｎビットを読み出して、送信データm_Aと受信データm_Bを生成する。本実施の形態では、残ったデータのビット位置が、送信側の通信装置と受信側の通信装置との間で共有できている。なお、m_Bは、上記m_b同様、確率情報付きの硬判定値である。

つぎに、送信側の通信装置では、シンドローム生成部１４が、パリティ検査行列Ｈ（ｎ×ｋ行列）と巡回符号ＣＲＣ（ｎ×ｄ行列）とを連結し、連結後の行列と送信データm_Aとを用いて、m_Aのシンドローム$S_A=H\times m_A$および巡回符号シンドローム$S_C=CRC\times m_A$を計算し、その結果を、公開通信路通信部１３，公開通信路を介して受信側の通信装置に通知する（ステップＳ５）。第８図は、m_AのシンドロームS_Aおよび巡回符号シンドロームS_Cの生成方法の概略構成を示す図である。この段階で、m_AのシンドロームS_A（ｋビット分の情報）および巡回符号シンドロームS_C（ｄビット分の情報）は盗聴者に知られる可能性がある。一

方、受信側の通信装置では、公開通信路通信部３４にてm_AのシンドロームS_Aおよび巡回符号シンドロームS_Cを受信し、それをシンドローム復号部３３に通知する（ステップＳ１４）。

つぎに、シンドローム復号部３３では、本実施の形態のシンドローム復号法を用いて、元の送信データm_Aを推定する（ステップＳ１５）。詳細には、雑音等による確率情報付きの硬判定値m_Bの誤りを訂正することによって推定後m_Cを生成し、推定後m_Cに誤りがなければそれを元の送信データm_Aと判定する。ここでは、「$S_A = Hm_C$」を満たすm_Cを確率情報付きの硬判定値m_Bから推定し、その推定結果m_Cに誤りがなければそれを共有情報m_Aとする。以下、本実施の形態のシンドローム復号法を詳細に説明する。

第９図は、本実施の形態のシンドローム復号法を示すフローチャートである。なお、上記のように、２元のｎ（列）×ｋ（行）の検査行列Ｈを想定した場合、ｉ列（$1 \leqq i \leqq n$）ｊ行（$1 \leqq j \leqq k$）目の要素をH_{ij}と表記する。また、受信データm_Bを$m_B = (m_{B1}, m_{B2}, \cdots, m_{Bn})$とし、推定語（硬判定値）$m_C$を$m_C = (m_{C1}, m_{C2}, \cdots, m_{Cn})$とする。また、$m_A$のシンドローム$S_A$を$S_A = (S_{A1}, S_{A2}, \cdots, S_{Ak})$、また、通信路としては、条件付確率$P(m_B \mid m_C = m_A)$で記述される無記憶通信路を想定する。

まず、シンドローム復号部３３では、初期設定として、$H_{ij} = 1$を満たす全ての列と行の組み合わせ（ｉ，ｊ）の事前値を$q_{ij}(0) = 1/2$，$q_{ij}(1) = 1/2$とする。$q_{ij}(0)$はH_{ij}が「０」である確率を表し、$q_{ij}(1)$はH_{ij}が「１」である確率を表す。そして、復号の反復回数を示すカウンタ値を$l = 1$（イテレーション：１回）とし、さらに、最大反復回数l_{max}を設定する（ステップＳ３１）。

つぎに、シンドローム復号部３３では、ｊ＝１，２，…，ｋの順に、$H_{ij} = 1$を満たす全ての列と行の組み合わせ（ｉ，ｊ）について外部値$r_{ij}(0)$と$r_{ij}(1)$を更新する（ステップＳ３２）。本実施の形態においては、たとえば、ｊ（$1 \leqq j \leqq k$）番目のシンドロームS_{Aj}が「０」の場合、更新式（６），更新式

（７）を用いて外部値r_{ij}（０）とr_{ij}（１）を更新する。

$$r_{ir}(0)=K\times\Sigma(\prod q_{i'j}(m_{Ci'})P(m_{Bi'}|m_{Ci'}))$$
$$M_{Ci'}\in 0,1 \qquad \cdots (6)$$
$$\Sigma M_{Ci'}=0$$
$$i'\in A(i)\setminus j$$

$$r_{ir}(1)=K\times\Sigma(\prod q_{i'j}(m_{Ci'})P(m_{Bi'}|m_{Ci'}))$$
$$M_{Ci'}\in 0,1 \qquad \cdots (7)$$
$$\Sigma M_{Ci'}=1$$
$$i'\in A(i)\setminus j$$

一方、ｊ（１≦ｊ≦ｋ）番目のシンドロームＳ$_{Aj}$が「１」の場合は、更新式（８），更新式（９）を用いて外部値r_{ij}（０）とr_{ij}（１）を更新する。

$$r_{ir}(0)=K\times\Sigma(\prod q_{i'j}(m_{Ci'})P(m_{Bi'}|m_{Ci'}))$$
$$M_{Ci'}\in 0,1 \qquad \cdots (8)$$
$$\Sigma M_{Ci'}=1$$
$$i'\in B(j)\setminus i$$

$$r_{ir}(1)=K\times\Sigma(\prod q_{i'j}(m_{Ci'})P(m_{Bi'}|m_{Ci'}))$$
$$M_{Ci'}\in 0,1 \qquad \cdots (9)$$
$$\Sigma M_{Ci'}=0$$
$$i'\in B(j)\setminus i$$

なお、上記Ｋは、「r_{ij}（０）＋r_{ij}（１）＝１」が成り立つように規定された値（正規化するための値）とする。また、上記Ｐ（m_B｜m_C）は、条件付確率、すなわち、推定語m_Cが「０」または「１」の場合における受信データm_Bの確率を表す。また、上記部分集合Ａ（ｉ）は、検査行列Ｈのｉ列目において「１」が立っている行インデックスの集合を表し、部分集合Ｂ（ｊ）は、検査行列Ｈのｊ行目において「１」が立っている列インデックスの集合を表す。

上記更新処理を具体的に記載すると、たとえば、$S_{Aj}=0$，$j=1$，かつ$H_{i1}=1$を満たす全ての列と行の組み合わせが（i，1）＝（3，1）（4，1）（5，1）の場合、式（6），式（7）が適用され、外部値$r_{31}(0)$，$r_{31}(1)$が式（10），式（11）のように更新される。すなわち、H_{31}以外のH_{41}，H_{51}を用いて、外部値$r_{31}(0)$，$r_{31}(1)$を更新する。ここでは、検査行列Hの3列1行目が「0」である確率と「1」である確率をそれぞれ求めている。

$$\begin{aligned} r_{31}(0) = K \times \{ & q_{41}(m_{C4}=0)\, P(m_{B4}|m_{C4}=0) \\ & \times q_{51}(m_{C5}=0)\, P(m_{B5}|m_{C5}=0) \\ & + q_{41}(m_{C4}=1)\, P(m_{B4}|m_{C4}=1) \\ & \times q_{51}(m_{C5}=1)\, P(m_{B5}|m_{C5}=1)\} \end{aligned} \quad \cdots (10)$$

$$\begin{aligned} r_{31}(1) = K \times \{ & q_{41}(m_{C4}=1)\, P(m_{B4}|m_{C4}=1) \\ & \times q_{51}(m_{C5}=0)\, P(m_{B5}|m_{C5}=0) \\ & + q_{41}(m_{C4}=0)\, P(m_{B4}|m_{C4}=0) \\ & \times q_{51}(m_{C5}=1)\, P(m_{B5}|m_{C5}=1)\} \end{aligned} \quad \cdots (11)$$

つぎに、シンドローム復号部33では、$i=1$，2，…，nの順に、$H_{ij}=1$を満たす全ての列と行の組み合わせ（i，j）について事前値$q_{ij}(0)$と$q_{ij}(1)$を更新する（ステップS33）。この更新処理は、式（12），式（13）にて表すことができる。

$$q_{ij}(0) = K' \times \prod_{j'=A(i)\setminus j} r_{ij'}(0) \quad \cdots (12)$$

$$q_{ij}(1) = K' \times \prod_{j'=A(i)\setminus j} r_{ij'}(1) \quad \cdots (13)$$

なお、上記K´は、「$q_{ij}(0)+q_{ij}(1)=1$」が成り立つように規定され

た値（正規化するための値）とする。

上記更新処理を具体的に記載すると、たとえば、ｉ＝３，かつH_{1j}＝１を満たす全ての列と行の組み合わせが（３，ｊ）＝（３，１）（３，２）（３，３）の場合、式（１２），式（１３）が適用され、事前値q_{31}（０），q_{31}（１）が式（１４），式（１５）のように更新される。すなわち、H_{31}以外のH_{32}，H_{33}を用いて、事前値q_{31}（０），q_{31}（１）を更新する。

$$q_{31}(0)=K'\times\{r_{32}(0)\times r_{33}(0)\} \quad \cdots (14)$$

$$q_{31}(1)=K'\times\{r_{32}(1)\times r_{33}(1)\} \quad \cdots (15)$$

つぎに、シンドローム復号部３３では、事後確率（条件付確率×事前値）Q_i（０），Q_i（１）を求め、この事後確率から一時推定語m_C'＝（m_{C1}'，m_{C2}'，…，m_{Cn}'）を求める（ステップＳ３４）。すなわち、式（１６），式（１７）の計算結果に基づいて、式（１８）における一時推定語を得る。ここでは、イテレーション１回毎に判定処理を行う。

$$Q_i(0)=K''\times P(m_{Bi}|m_{Ci}=0)\prod_{j'\in A(i)} r_{ij'}(0) \quad \cdots (16)$$

$$Q_i(1)=K''\times P(m_{Bi}|m_{Ci}=1)\prod_{j'\in A(i)} r_{ij'}(1) \quad \cdots (17)$$

$$m_{Ci}'=\begin{cases}0:\text{if } Q_i(0)\geq Q_i(1)\\ 1:\text{if } Q_i(0)<Q_i(1)\end{cases} \quad \cdots (18)$$

なお、上記K''は、「Q_i（０）＋Q_i（１）＝１」が成り立つように規定された値（正規化するための値）とする。また、条件付確率Ｐ（m_B｜m_C＝０）は、

式（１９），式（２０）のように定義され、ｐはビット誤り率を表す。

$$P(m_{Bi'}|m_{Ci'}=0)=\begin{cases}1-p\,(m_{Bi'}=0)\\ p\,(m_{Bi'}=1)\end{cases} \quad \cdots (19)$$

$$P(m_{Bi'}|m_{Ci'}=1)=\begin{cases}p\,(m_{Bi'}=0)\\ 1-p\,(m_{Bi'}=1)\end{cases} \quad \cdots (20)$$

つぎに、シンドローム復号部３３では、一時推定語$m_C{}'$が送信データm_Aといえるかどうかを検査する（ステップＳ３５）。ここでは、たとえば、$m_C{}'=(m_{C1}{}', m_{C2}{}', \cdots, m_{Cn}{}')$が「$m_C{}' \times H^T = S_A$」という条件を満たしていれば（ステップＳ３６、Ｙｅｓ）、当該$m_C{}'$を推定語$m_C=(m_{C1}, m_{C2}, \cdots, m_{Cn})$として出力する。

一方、上記条件を満たさない場合で、かつ$l < l_{max}$の場合は（ステップＳ３６、Ｎｏ）、カウンタ値ｌをインクリメントし、ステップＳ３２の処理を上記更新された値を用いて再度実行する。以降、上記条件を満たすまで（$l < l_{max}$の範囲で）、更新された値を用いてステップＳ３２～Ｓ３６の処理を繰り返し実行する。

つぎに、シンドローム復号部３３では、上記推定語$m_C=(m_{C1}, m_{C2}, \cdots, m_{Cn})$と、受信データ$m_B=(m_{B1}, m_{B2}, \cdots, m_{Bn})$と、を比較（ＥＸＯＲ）し、エラーベクトル（受信データ$m_B=m_A+e$（雑音等）のｅに相当）を出力する（ステップＳ３７）。

つぎに、シンドローム復号部３３では、「$H \times m_C = S_A$」を満たす推定後m_Cが複数個存在すること（ＨとS_Aを固定した場合のm_Cのエントロピーは2^{n-k}個となる）が原因で誤判定が発生し、送信データm_Aを正確に推定できない可能性（送信データm_Aと上記で正しいと判定した推定語m_Cが一致しない場合）があることから、上記推定語m_Cの誤り検出を行う（ステップＳ３８）。ここでは、上記ステップＳ１４にて受信した巡回符号シンドローム$S_C=CRC \times m_A$と、式（２１）に示す推定巡回符号シンドローム$S_C{}'$と、を比較し、$S_C=S_C{}'$であれば、推定語m_C

に誤りがないと判断し、上記推定語m_C＝（m_{C1}，m_{C2}，…，m_{Cn}）を元の送信データm_A＝（m_{A1}，m_{A2}，…，m_{An}）として出力し、第９図に示すアルゴリズムを終了する。一方で、$S_C \neq S_C'$であれば、推定語m_Cに誤りがあると判断し、この推定語m_Cを捨てる。

$$S_C' = rem(m_C / gx) \quad \cdots (21)$$

ただし、上記ｒｅｍは、ＧＦ（２）上の除算m_C / gxの剰余を表す。

このように、上記本実施の形態の量子鍵配送で採用するシンドローム復号法においては、従来技術にて記載した誤り訂正で発生していた「エラービットを特定するための膨大な回数のパリティのやりとり（二分探索）」を排除し、極めて高い特性（誤り訂正能力）をもつＬＤＰＣ符号用のパリティ検査行列を用いて誤り訂正を行うこととした。これにより、短時間で伝送路上におけるデータ誤りを訂正しつつ、高度に安全性の保証された共通鍵を生成することができる。

また、本実施の形態では、送信側の通信装置が生成した巡回符号シンドロームS_Cと、推定語m_Cに基づいて生成した推定巡回符号シンドロームS_C'と、を比較し、推定語m_Cの誤り検出を行うこととした。これにより、受信データm_Bから判定した推定語m_Cの誤判定確率を大幅に低減することができる。すなわち、元の送信データm_Aを高精度に推定できる。

なお、本実施の形態においては、受信データm_Bおよびm_bを確率情報付きの硬判定値としたが、これに限らず、たとえば、軟判定値としてもよい。

上記のように送信データm_Aを推定後、最後に、受信側の通信装置では、共有鍵生成部３５が、公開された誤り訂正情報（盗聴された可能性のある上記ｋビット分の情報：S_A）に応じて共有情報（m_A）の一部を捨てて、ｎ－ｋビット分の情報量を備えた暗号鍵ｒを生成する（第３図、ステップＳ１６）。すなわち、共有鍵生成部３５では、先に計算しておいたG^{-1}（ｎ×（ｎ－ｋ））を用いて下記（２２）式により暗号鍵ｒを生成する。受信側の通信装置は、この暗号鍵ｒを送信側の通信装置との共有鍵とする。

$$r = G^{-1} m_A \quad \cdots (22)$$

一方で、送信側の通信装置においても、共有鍵生成部１５が、公開された誤り訂正情報（盗聴された可能性のある上記ｋビット分の情報：S_A）に応じて共有情報（m_A）の一部を捨てて、ｎ－ｋビット分の情報量を備えた暗号鍵ｒを生成する（第２図、ステップＳ６）。すなわち、共有鍵生成部１５では、先に計算しておいたG^{-1}（ｎ×（ｎ－ｋ））を用いて上記（２２）式により暗号鍵ｒを生成する（ステップＳ６）。送信側の通信装置は、この暗号鍵ｒを受信側の通信装置との共有鍵とする。

なお、本実施の形態においては、さらに、正則なランダム行列Ｒを用いて上記共有鍵を並べ替える構成としてもよい。これにより、秘匿性を増強させることができる。具体的には、まず、送信側の通信装置が、正則なランダム行列Ｒ（（ｎ－ｋ）×（ｎ－ｋ））を生成し、さらに、当該Ｒを、公開通信路を介して受信側の通信装置に通知する。ただし、この処理は、受信側の通信装置で行うこととしてもよい。その後、送信側および受信側の通信装置が、先に計算しておいたG^{-1}（ｎ×（ｎ－ｋ））とランダム行列Ｒを用いて下記（２３）式により暗号鍵ｒを生成する。

$$r = RG^{-1}m_A \qquad \cdots (23)$$

以上、本実施の形態おいては、確定的で特性が安定した「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」用のパリティ検査行列を用いて共有情報のデータ誤りを訂正し、さらに、巡回符号ＣＲＣを用いて共有情報（推定語）の誤り検出を行い、その後、公開された誤り訂正情報に応じて共有情報の一部を捨てる構成とした。これにより、エラービットを特定／訂正するための膨大な回数のパリティのやりとりがなくなり、誤り訂正情報を送信するだけで誤り訂正制御が行われるため、誤り訂正処理にかかる時間を大幅に短縮できる。

また、本実施の形態においては、送信側の通信装置が生成した誤り検出情報を用いて、受信側の通信装置が推定語の誤り検出を行うこととした。これにより、推定語の誤判定確率を大幅に低減することができ、元の送信データを高精度に推定できる。

また、本実施の形態においては、公開された情報に応じて共有情報の一部を捨てているので、高度に安全性の保証された共通鍵を生成することができる。

なお、本実施の形態では、$HG=0$を満たす生成行列G（（n－k）×n）から、$G^{-1}\cdot G=I$（単位行列）となる逆行列G^{-1}（n×（n－k））を生成し、当該逆行列G^{-1}を用いて共有情報（n）の一部（k）を捨てて、n－kビット分の情報量を備えた暗号鍵rを生成することとしたが、これに限らず、共有情報（n）の一部を捨てて、m（m≦n－k）ビット分の情報量を備えた暗号鍵rを生成することとしてもよい。具体的にいうと、n次元ベクトルをm次元ベクトルに写す写像F（・）を想定する。F（・）は、共有鍵の安全性を保証するために、「任意のm次元ベクトルvに対して、写像Fと生成行列Gの合成写像F・Gにおける逆像$(F\cdot G)^{-1}(v)$の元の個数がvによらず一定(2^{n-k-m})である」、という条件を満たす必要がある。このとき、共有鍵rは、$r=F(m_A)$となる。

また、本実施の形態においては、ステップＳ６，Ｓ１６の処理で、生成行列G^{-1}を用いずに、パリティ検査行列Hの特性を用いて共有情報の一部を捨てる構成としてもよい。具体的には、まず、共有鍵生成部１５，３５が、上記ステップＳ１，Ｓ１１で生成したパリティ検査行列Hの列に対してランダム置換を行う。そして、通信装置間で捨てるビットに関する情報を、公開通信路を介して交換する。たとえば、元の有限アフィン幾何ＡＧ（２，2^s）の１列目の中から特定の「１」を選び、その位置を、公開通信路を介して交換する。その後、共有鍵生成部１５，３５が、上記置換後のパリティ検査行列から上記「１」に対応する分割後の位置、および巡回シフトされた各列における上記「１」に対応する分割後の位置を特定し、その特定した位置に対応する共有情報m_A内のビットを捨てて、残りのデータを暗号鍵rとする。これにより、複雑な生成行列G，G^{-1}の演算処理を削除することができる。

産業上の利用可能性

以上のように、本発明にかかる量子鍵配送方法および通信装置は、高度に安全

性の保証された共通鍵を生成する技術として有用であり、特に、盗聴者が存在する可能性のある伝送路上の通信に適している。

請　求　の　範　囲

1．　暗号鍵の元となる乱数列を所定の量子状態で量子通信路上に送信する送信側の通信装置と、当該量子通信路上の光子を測定する受信側の通信装置、で構成された量子暗号システムにおける量子鍵配送方法において、

各通信装置が、同一のパリティ検査行列（要素が「０」または「１」の行列）を生成する検査行列生成ステップと、

前記送信側の通信装置が、誤り検出のための巡回符号（ＣＲＣ：Cyclic Redundancy check）を生成する巡回符号生成ステップと、

前記受信側の通信装置が、光方向を正しく識別可能な測定器で測定した結果として得られた確率情報付きの受信データを保持し、前記送信側の通信装置が、前記受信データに対応する送信データ（乱数列の一部）を保持する送受信ステップと、

前記送信側の通信装置が、前記パリティ検査行列および前記送信データに基づいて生成した誤り訂正情報と、前記巡回符号および前記送信データに基づいて生成した誤り検出情報と、を公開通信路を介して前記受信側の通信装置に通知する情報通知ステップと、

前記受信側の通信装置が、前記パリティ検査行列と前記確率情報付きの受信データと前記誤り訂正情報と前記誤り検出情報に基づいて、前記送信データを推定する送信データ推定ステップと、

前記各通信装置が、公開された情報量に応じて送信データの一部を捨てて、残りの情報で暗号鍵を生成する暗号鍵生成ステップと、

を含むことを特徴とする量子鍵配送方法。

2．　前記送信データ推定ステップにあっては、

初期設定として、前記パリティ検査行列内の要素「１」に対応する事前値を設定する初期設定ステップと、

前記誤り訂正情報に応じて、前記パリティ検査行列内の要素「１」に対応する外部値を、同一行における他の要素「１」に対応する事前値および前記確率情報を用いて更新する処理、を行単位に実行する外部値更新ステップと、

前記パリティ検査行列内の要素「１」に対応する事前値を、同一列における他の要素「１」に対応する前記更新後の外部値を用いて更新する処理、を列単位に実行する事前値更新ステップと、

前記確率情報および前記更新後の事前値に基づいて事後確率を算出し、当該事後確率から一時推定語を求める（硬判定）一時推定ステップと、

前記一時推定語が前記パリティ検査行列との間に確立されている所定の条件を満たす場合に、前記誤り検出情報を用いて当該一時推定語の誤り検出を行い、誤りがなければ当該一時推定語を元の送信データと判定し、前記所定の条件を満たさない場合に、当該条件を満たすまで前記更新後の値を用いて、前記外部値更新ステップ、前記事前値更新ステップおよび前記一時推定ステップを繰り返し実行する送信データ推定ステップと、

を含むことを特徴とする請求の範囲第１項に記載の量子鍵配送方法。

３．　前記送信データ推定ステップにあっては、

前記誤り検出情報と、前記一時推定語を用いて生成した推定誤り検出情報と、を比較し、一致していれば前記一時推定語に誤りがないと判断し、一致していなければ前記一時推定語に誤りがあると判断することを特徴とする請求の範囲第２項に記載の量子鍵配送方法。

４．　量子鍵配送により装置間で暗号鍵を共有する量子暗号システムを構成し、かつ暗号鍵の元となる乱数列を所定の量子状態で量子通信路上に送信する通信装置において、

暗号鍵を共有する相手側装置と同一のパリティ検査行列を生成するパリティ検査行列生成手段と、

誤り検出のための巡回符号（ＣＲＣ：Cyclic Redundancy check）を生成する巡回符号生成手段と、

光方向を正しく識別可能な測定器で測定した結果として得られる相手側装置の受信データに対応する送信データ（乱数列の一部）および前記パリティ検査行列に基づいて生成した誤り訂正情報と、前記送信データおよび前記巡回符号に基づいて生成した誤り検出情報と、を公開通信路を介して前記相手側装置に通知する情報通知手段と、

公開された情報量に応じて前記送信データの一部を捨てて、残りの情報で暗号鍵を生成する暗号鍵生成手段と、

を備えることを特徴とする通信装置。

５．　量子鍵配送により装置間で暗号鍵を共有する量子暗号システムを構成し、かつ量子通信路上の光子（暗号鍵の元となる乱数列）を測定する通信装置において、

暗号鍵を共有する相手側装置と同一のパリティ検査行列（要素が「０」または「１」の行列）を生成するパリティ検査行列生成手段と、

誤り検出のための巡回符号（ＣＲＣ：Cyclic Redundancy check）を生成する巡回符号生成ステップと、

前記パリティ検査行列、光方向を正しく識別可能な測定器で測定して得られた確率情報付きの受信データ、相手側装置から公開通信路を介して受信した誤り訂正情報および誤り検出情報に基づいて、元の送信データを推定する送信データ推定手段と、

公開された情報量に応じて前記送信データの一部を捨てて、残りの情報で暗号鍵を生成する暗号鍵生成手段と、

を備えることを特徴とする通信装置。

６．　前記送信データ推定手段は、

初期設定として、前記パリティ検査行列内の要素「１」に対応する事前値を設定し、

つぎに、前記誤り訂正情報に応じて、前記パリティ検査行列内の要素「１」に対応する外部値を、同一行における他の要素「１」に対応する事前値および前記確率情報を用いて更新する処理、を行単位に実行し、

つぎに、前記パリティ検査行列内の要素「１」に対応する事前値を、同一列における他の要素「１」に対応する前記更新後の外部値を用いて更新する処理、を列単位に実行し、

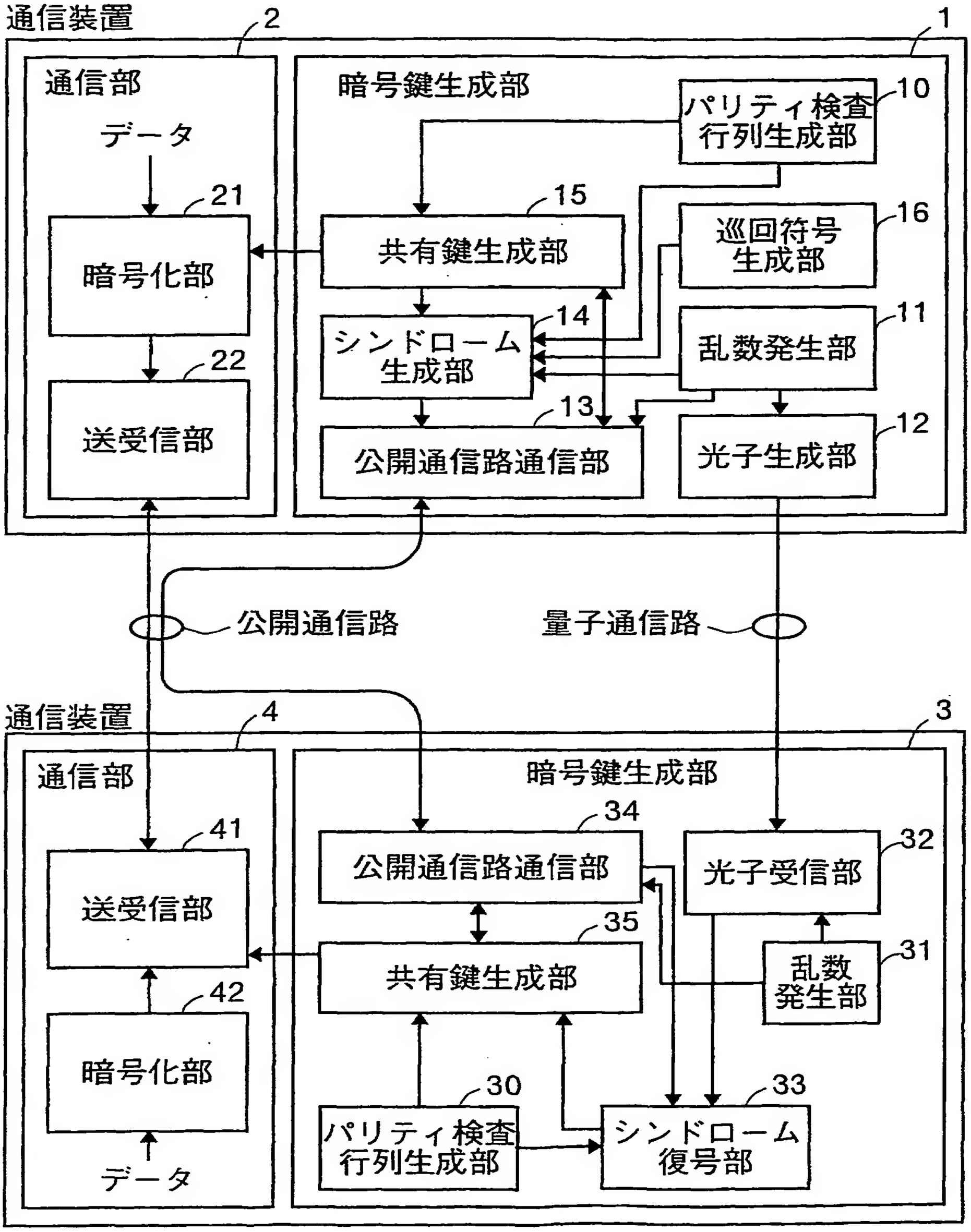
つぎに、前記確率情報および前記更新後の事前値に基づいて事後確率を算出し、当該事後確率から一時推定語を判定し、

つぎに、前記一時推定語が前記パリティ検査行列との間に確立されている所定の条件を満たす場合に、前記誤り検出情報を用いて当該一時推定語の誤り検出を行い、誤りがなければ当該一時推定語を元の送信データと判定し、前記所定の条件を満たさない場合に、当該条件を満たすまで前記更新後の値を用いて、前記行単位の処理、前記列単位の処理および前記一時推定語判定処理を繰り返し実行することを特徴とする請求の範囲第５項に記載の通信装置。

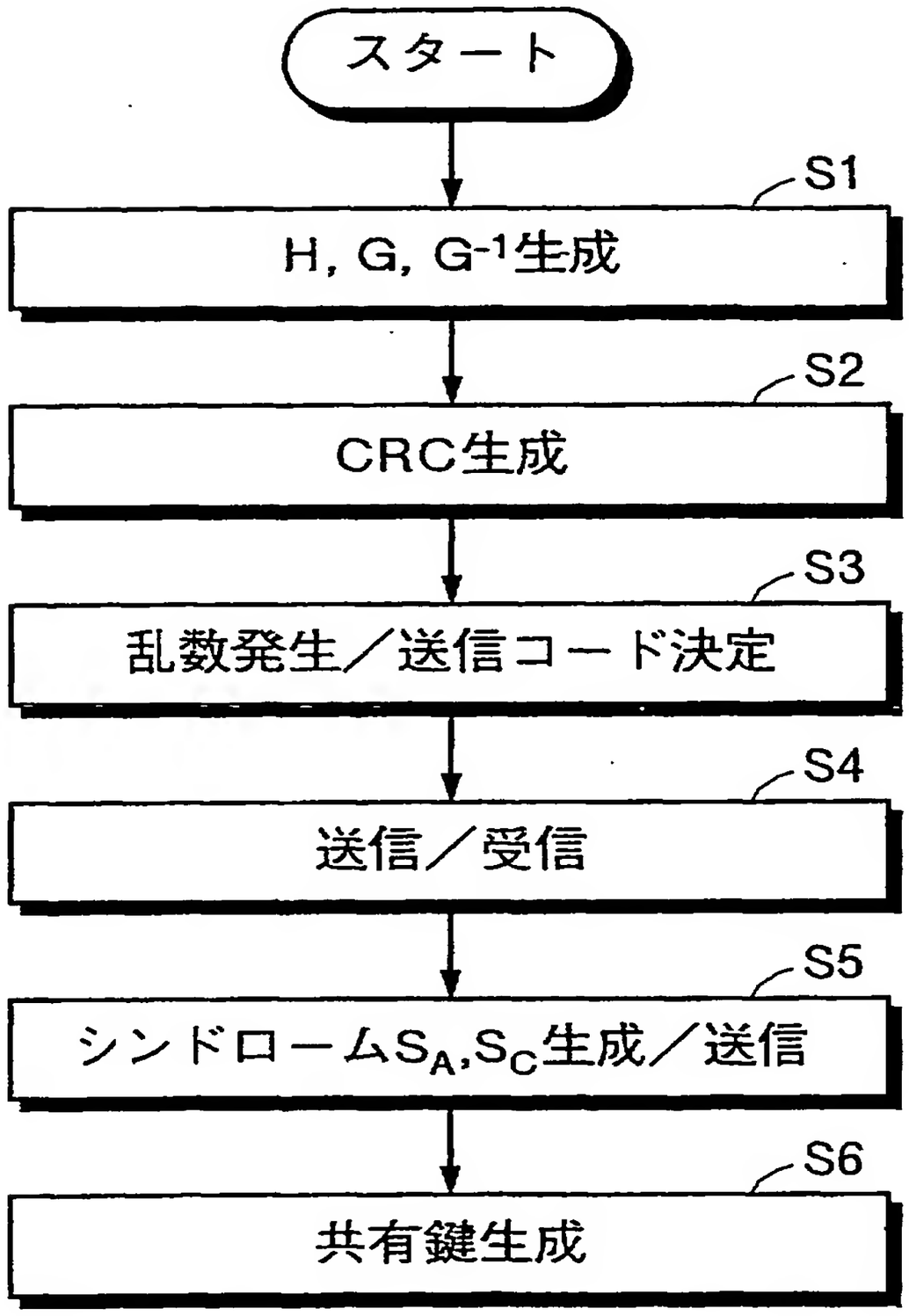
７．　前記送信データ推定手段は、

前記誤り検出情報と、前記一時推定語を用いて生成した推定誤り検出情報と、を比較し、一致していれば前記一時推定語に誤りがないと判断し、一致していなければ前記一時推定語に誤りがあると判断することを特徴とする請求の範囲第６項に記載の通信装置。

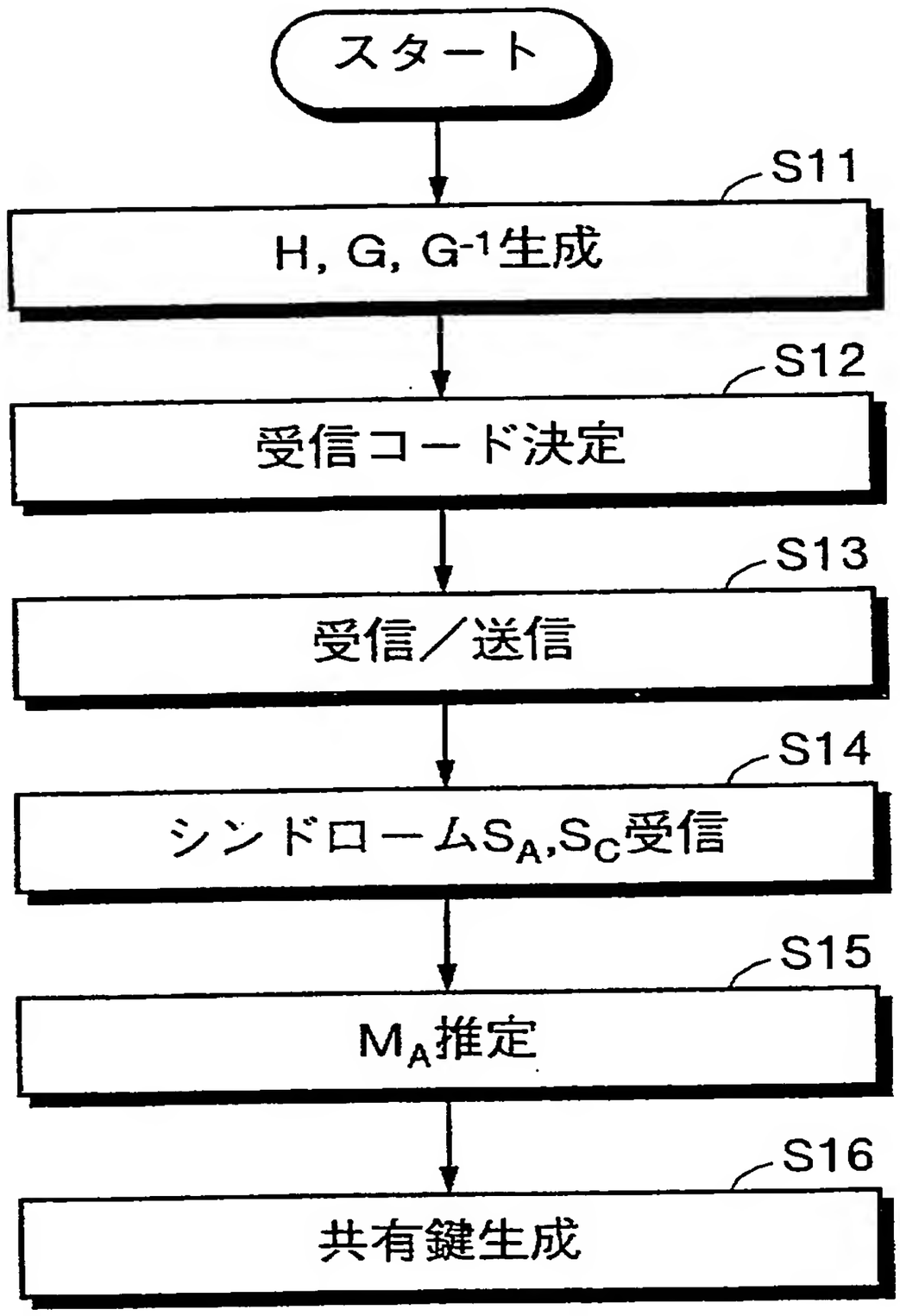
第1図


通信装置
2
1
通信部
データ
21
暗号化部
22
送受信部
暗号鍵生成部
10
パリティ検査
行列生成部
15
共有鍵生成部
16
巡回符号
生成部
14
シンドローム
生成部
11
乱数発生部
13
公開通信路通信部
12
光子生成部
公開通信路
量子通信路
通信装置
4
3
通信部
41
送受信部
42
暗号化部
データ
暗号鍵生成部
34
公開通信路通信部
32
光子受信部
35
共有鍵生成部
31
乱数
発生部
30
パリティ検査
行列生成部
33
シンドローム
復号部

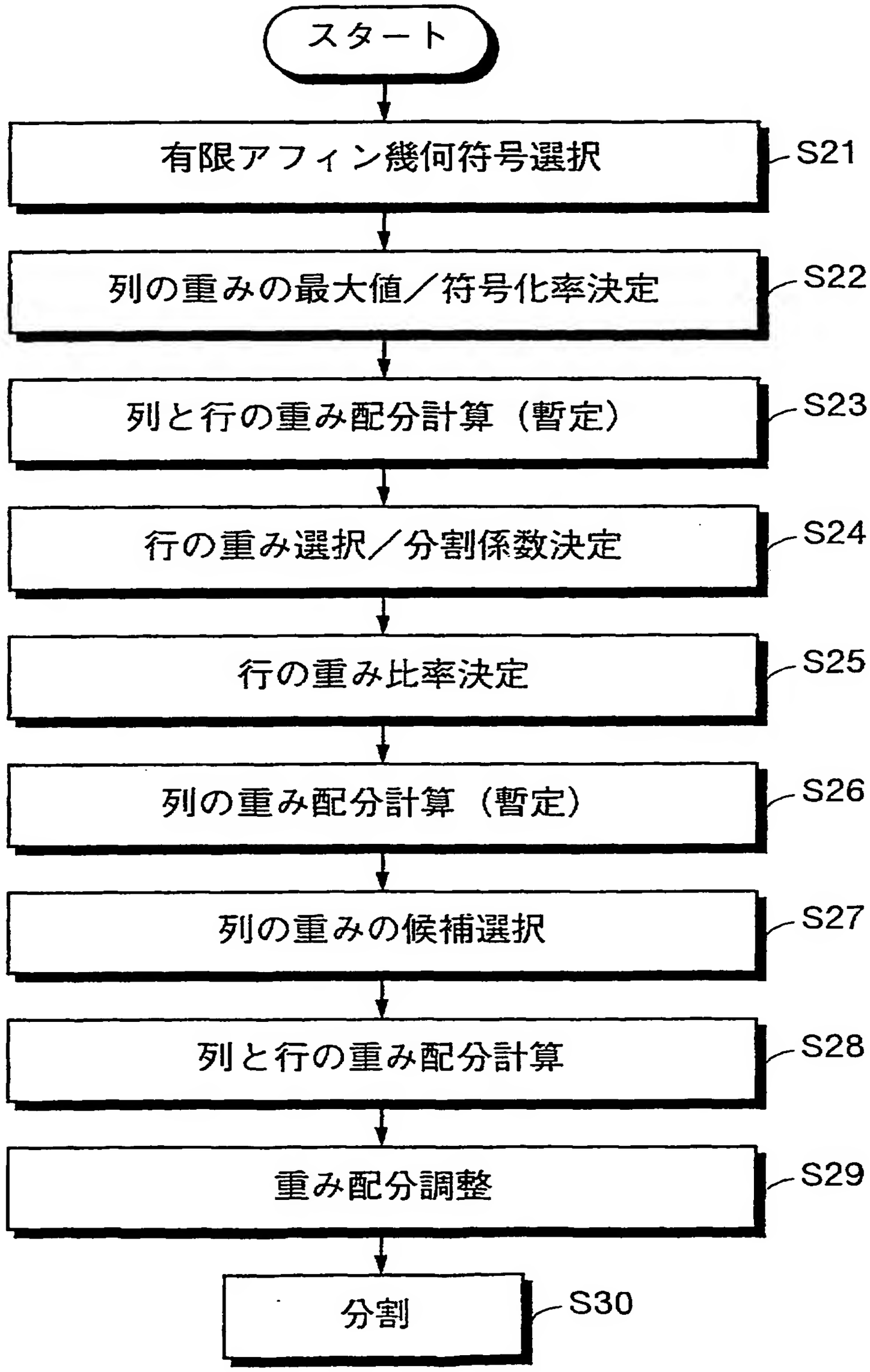
第2図


スタート
S1
H, G, G-1生成
S2
CRC生成
S3
乱数発生／送信コード決定
S4
送信／受信
S5
シンドロームSA,SC生成／送信
S6
共有鍵生成

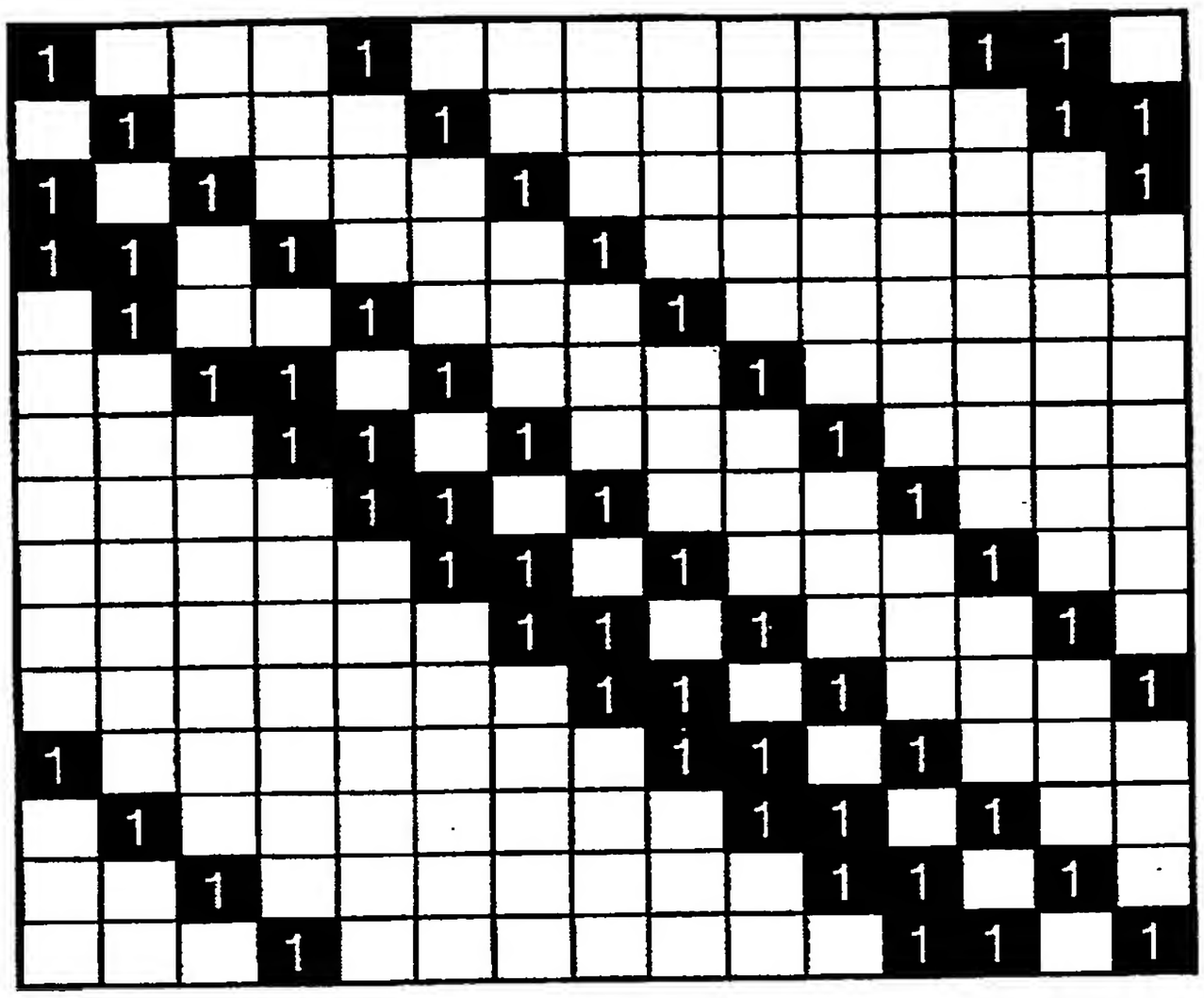
第3図


スタート
S11
H, G, G-1生成
S12
受信コード決定
S13
受信／送信
S14
シンドロームSA,SC受信
S15
MA推定
S16
共有鍵生成

第4図


スタート
有限アフィン幾何符号選択
S21
列の重みの最大値／符号化率決定
S22
列と行の重み配分計算（暫定）
S23
行の重み選択／分割係数決定
S24
行の重み比率決定
S25
列の重み配分計算（暫定）
S26
列の重みの候補選択
S27
列と行の重み配分計算
S28
重み配分調整
S29
分割
S30

第5図



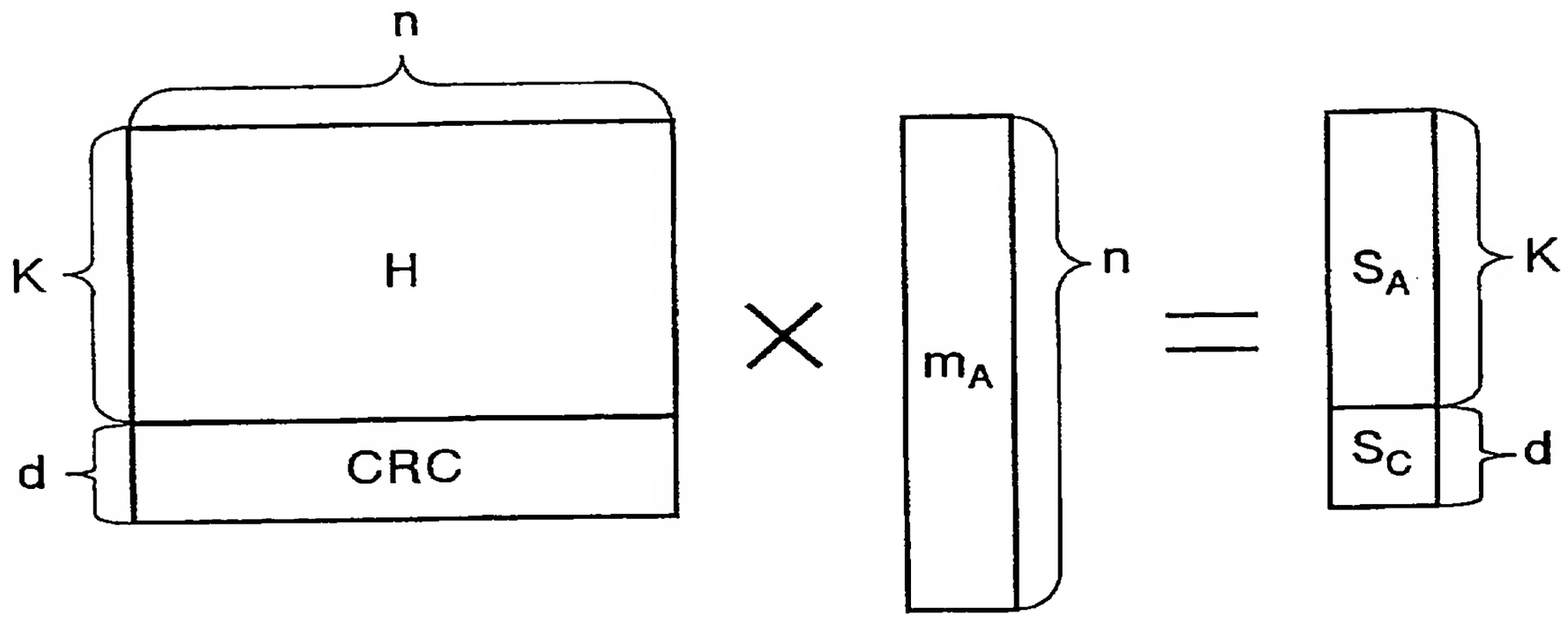
第6図

rate		0.5	
N		12.6	
i	γ_i	$\lambda(\gamma_i)$	$n(\gamma_i)$
1	2	0.27381	69
2	3	0.10714	18
3	8	0.61905	39
u		ρ_u	nu
8		1	63

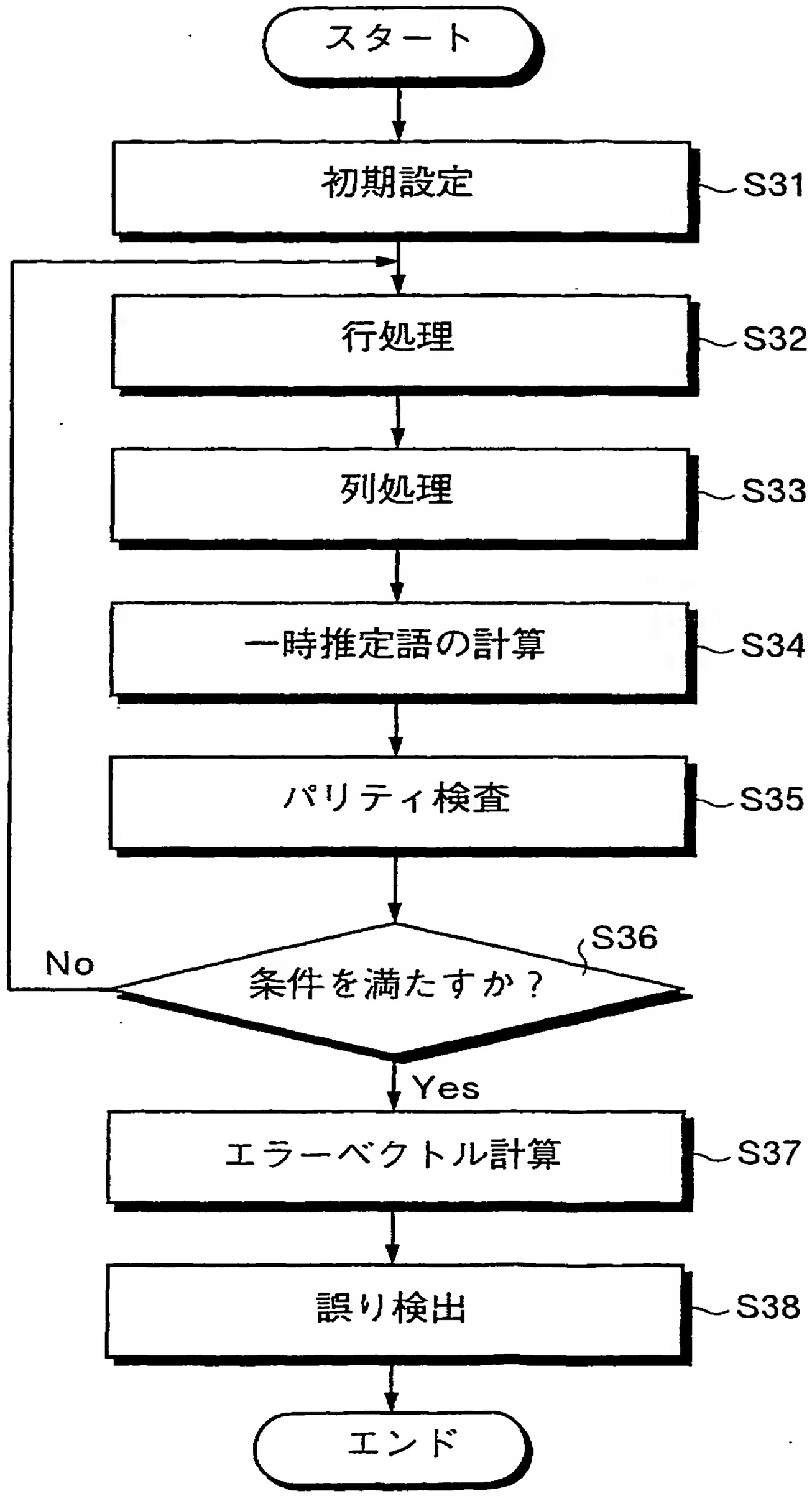
第7図

$$CRC = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

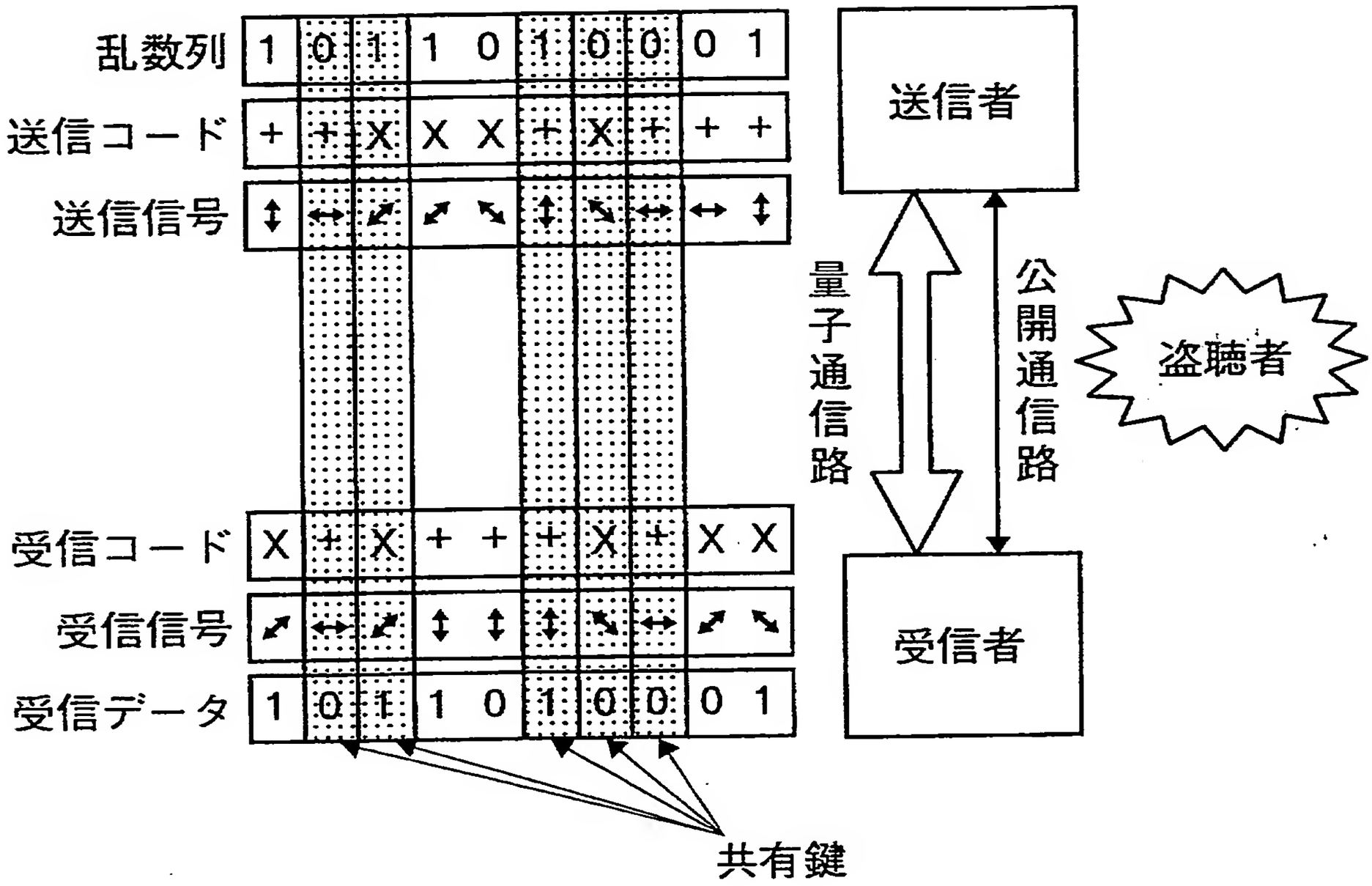
第8図



第9図


スタート
初期設定
S31
行処理
S32
列処理
S33
一時推定語の計算
S34
パリティ検査
S35
S36
No
条件を満たすか？
Yes
エラーベクトル計算
S37
誤り検出
S38
エンド

第10図


乱数列
1 0 1 1 0 1 0 0 0 1
送信コード
+ + X X X + X + + +
送信信号
受信コード
X + X + + + X + X X
受信信号
受信データ
1 0 1 1 0 1 0 0 0 1
共有鍵
送信者
受信者
量子通信路
公開通信路
盗聴者